U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

December 5, 2016

FILED BY ECF AND BY HAND
The Honorable Richard M. Berman
United States District Judge
Daniel Patrick Moynihan U.S. Courthouse
500 Pearl Street
New York, New York 10007

Re: United States v. Reza Zarrab, a/k/a "Riza Sirraf,"
S2 15 Cr. 867 (RMB)

Dear Judge Berman:

The Government respectfully submits this letter pursuant to the Court's request at the *Curcio* hearing held on November 30, 2016, for an outline, including citations, of the Government's argument with respect to the inevitable discovery of the contents of the defendant's email account. If the Court determines that the defendant has met the high burden to hold a *Franks* hearing in this case, the Government requests the opportunity to supplement this briefing and factual record as appropriate.

Applicable Law

"Under the 'inevitable discovery' doctrine, evidence obtained during the course of an unreasonable search and seizure should not be excluded 'if the government can prove that the evidence would have been obtained inevitably' without the constitutional violation." *United States* v. *Heath*, 455 F.3d 52, 55 (2d Cir.2006) (quoting *Nix* v. *Williams*, 467 U.S. 431, 447 (1984)). "To prevail under the inevitable discovery doctrine, . . . the government must prove that each event leading to the discovery of the evidence would have occurred with a sufficiently high degree of confidence for the district judge to conclude, by a preponderance of the evidence, that the evidence would inevitably have been discovered." *United States* v. *Vilar*, 729 F.3d 62, 84 (2d Cir. 2013).

To satisfy this burden, the Government must prove by a preponderance of the evidence first that "active and ongoing investigation . . . was in progress at the time of unlawful search." *United States* v. *Eng*, 971 F.2d 854, 862 (2d Cir. 1992). If that prong is satisfied, the Court must then "determine what would have happened had the government misconduct never occurred, in light of what the government knew and was pursuing at the moment before the unlawful search, and other relevant facts and circumstances." *Id.* This analysis requires more than a right for the Government to seek a later, lawful search warrant, it also requires "confidence that law enforcement officers . . . would have done so under the circumstances," *Heath*, 455 F.3d at 60, and that "the issuance of a valid warrant was, under the circumstances, truly inevitable," *id* at 59 n.7. "[P]roof of inevitable discovery 'involves no speculative elements but focuses on

demonstrated historical facts capable of ready verification or impeachment and does not require a departure from the usual burden of proof at suppression hearings.'" *Eng*, 971 F.2d at 859 (quoting *Nix*, 467 U.S. at 444 n. 5).

Discussion

The Government easily meets this burden in this case. First, there is no question that there was an "active and ongoing investigation" of Zarrab at the time the affidavit in support of the warrant to search his email account was submitted in September 2014 (the "September 2014 Affidavit," *see* Sealed Exhibit A). As that affidavit makes clear, the Government had already focused on the significance of Zarrab's email account and had both subpoenaed records pertaining to the account (Sealed Exhibit A ¶ 24(c)), and obtained judicial orders for the installation of a pen register on that account (Sealed Exhibit A ¶ 25). The Government also had obtained a court order for the production of header information for emails stored in the account.

Even if the Government had not obtained a warrant to search the defendant's email account, the September 2014 warrant authorized the Government to search other email accounts for evidence related to the charged offenses, searches which resulted in overwhelming probable cause to search the defendant's email account. [1] *See Heath*, 455 F.3d at 59 n.7 ("[O]verwhelming probable cause is sufficient to find inevitable discovery," but it is "not . . . necessary to reach such a conclusion.").

For example, a search was made of the account "alnafees99@yahoo.com" (the "Al Nafees 99 Account"), an account registered in approximately June 2009 from an IP address that resolves to the United Arab Emirates, and the account "alnafees1999@yahoo.com" (the "Al Nafees 1999 Account"), an account registered in approximately October 2013 from an IP address that resolves to the United Arab Emirates with a user name provided as "ALNAFEES EXCHANGE," both of which were used to conduct business for Al Nafees Exchange. These emails show, among other things, that Al Nafees Exchange conducted international U.S. dollar financial transactions on behalf of and for the benefit of Iranian clients, such as Mellat Exchange, that were executed through correspondent accounts held at banks located in the United States; that Al Nafees Exchange conducted international financial transactions in U.S. dollars and foreign currencies for the benefit of and on behalf of Iranian entities, including entities designated as Specially Designated Nationals ("SDNs") by the U.S. Department of the Treasury, Office of Foreign Assets Control ("OFAC"); that Al Nafees Exchange conducted huge volumes of U.S. dollar international financial transfers and currency exchanges; and that Al Nafees Exchange communicated regularly with Zarrab and with Royal Holdings employees concerning international financial transactions, precious metals transactions, and currency transactions.

[1] The defendant has not objected, and does not have standing to object, to the searches of these other accounts. *United States* v. *Lustyik*, 57 F. Supp. 3d 213, 223 (S.D.N.Y. 2014) ("A person has no expectation of privacy in another person's email account."). Accordingly, even if the Court were to conclude both that suppression of the results of the search of the defendant's account was required by *Franks* and that the inevitable discovery doctrine did not apply, any of the defendant's emails recovered from the independent searches of other email accounts would still be admissible.

The Al Nafees 99 Account sent or received at least approximately 95 emails reflecting communications sent to or by the defendant's email account and which predated the September 2014 search warrant, and the Al Nafees 1999 Account sent or received at least approximately 10 additional such emails. Included in these emails were, among others:

- Numerous emails reflecting financial transactions with, for, or on behalf of Iranian banks, including banks identified by the U.S. Department of the Treasury, Office of Foreign Assets Control ("OFAC") as Specially Designated Nationals ("SDNs"). For example, Al Nafees Exchange sent the defendant documents reflecting multi-million-quantity deposits of UAE dirham by Al Nafees Exchange into accounts held at Bank Melli Iran and Bank Saderat—each an SDN at the time[2]—for other Iranian banks, including Bank Pasargad, Bank Parsian, and Bank Sarmayeh—each also an SDN at the time.[3] Zarrab's employee and co-defendant, Camellia Jamshidy, was copied on many of these documents.

- Emails reflecting Al Nafees Exchange's efforts to deliver multi-million-dollar packages of bulk cash to Tehran. For example, Al Nafees Exchange sent the defendant copies of correspondence from approximately March 2011 between Al Nafees Exchange and a Dubai-based transportation and security company concerning 100 kilogram shipments of U.S. dollars, totaling approximately $10 million, to Tehran and Istanbul. The defendant's account sent an email attaching a photograph of the defendant smiling and standing next to two stacks of large bundles of U.S. currency that stand several inches taller than the defendant's head.

- An email from December 2013 attaching a document listing 17 different amounts of U.S. dollars ranging from approximately $4,547,919 to $20 million and totaling

---

[2] Bank Melli Iran, a bank owned by the Government of Iran, was designated an SDN by OFAC on or about October 25, 2007 pursuant to the Weapons of Mass Destruction Proliferators Sanctions Regulations ("WMD Sanctions"). OFAC announced on March 12, 2008 that: "Bank Melli goes to extraordinary lengths to assist Iran's pursuit of a nuclear capability and ballistic missiles, while also helping other designated entities to dodge sanctions. . . . Banks and other entities owned or controlled by Bank Melli pose a serious threat to the integrity of the international financial system." Bank Melli has also, among other things, used shell companies to secretly own partnership interests in Manhattan commercial real estate. *See In re 650 Fifth Avenue and Related Properties*, 830 F.3d 66, 76-82 & 89-93 (2d Cir, 2016).

Bank Saderat Iran, another bank owned by the Government of Iran, was designated an SDN by OFAC on or about September 8, 2006, because of the role the bank played in Iran's support for foreign terrorist organizations. OFAC announced that: "Bank Saderat is one of the largest Iranian-owned banks, with roughly 3400 branch offices. The bank is used by the Government of Iran to transfer money to terrorist organizations, including Hizballah, Hamas, the Popular Front for the Liberation of Palestine-General Command and Palestinian Islamic Jihad. A notable example of this is a Hizballah-controlled organization that has received $50 million directly from Iran through Bank Saderat since 2001."

[3] Bank Pasargad, Bank Parsian, and Bank Sarmayeh each was identified by OFAC as an Iranian financial institution on or about July 12, 2012, and placed on the SDN list.

approximately $205,525,901, each amount having a corresponding date, along with two amounts of Euro totaling approximately € 22 million with corresponding dates. Handwritten at the top of the list, in Farsi, is the notation: "For the attention of Mr. Reza Zarrag: a list of [currency] parcels sent without invoices."

- Emails reflecting international financial transfers involving front companies used by Zarrab and Al Nafees Exchange to conduct international financial transactions, including Pirlanta in Turkey, Hicran General Trading in the UAE, and Anvil International General Trading in the UAE.[4]

- Emails reflecting that the defendant received information concerning Al Nafees Exchange's operations. For example, the defendant received an email showing foreign currency reserves and foreign currency transactions by Al Nafees Exchange, including large volumes of U.S. dollar transactions. The defendant also received an email attaching a letter from a Dubai bank requesting additional information concerning an inbound transfer of approximately 200 million UAE dirham to an Al Nafees Exchange account.

- An email reflecting financial transactions with the Sorinet Group, a business entity owned by financial sanctions evader Babak Zanjani. Al Nafees Exchange sent the defendant an email in April 2012 reflecting transfers totaling more than 42 million UAE dirham from a company called "Nadir Gold LLC" to "Sorinet General Trading," which appears to be part of Zanjani's Sorinet Group.

The searches of the Al Nafees 99 and Al Nafees 1999 accounts resulted in thousands of additional emails reflecting business conducted by Al Nafees Exchange with Zarrab or Zarrab's employees at Royal Holdings A.S. For example, the Al Nafees 99 Account contained more than 1800 emails reflecting communications to or from individuals with email accounts hosted at the domain name "@royaltk.com," an email domain used by employees and officers of Royal Holdings in Turkey. These emails contained some of the same information, or in some cases the same emails, described above that were sent to or received by Zarrab.

Also recovered from the Al Nafees 99 Account, *inter alia*, was the following:

- Between approximately January 2011 and October 2011, the email account [redacted] sent emails to the Al Nafees 99 Account containing documents concerning money transfers, including transfers of U.S. dollars, for Bank Mellat. At least approximately 21 of these U.S.-dollar transfers, totaling at least approximately $3,291,346.70, correspond to wire transfers processed through

[4] The Turkish Investigative Report describes "Pirlanta Ltd." as a Royal Holdings company used to produce and export gold in partnership with an Iranian entity. The Report also describes "Hicran Jewelry" as a company used by Zarrab and Happani, among other companies, to make it appear that gold was being exported to Iran, Saudi Arabia and Iraq but in realty were used to launder proceeds of drug trafficking and organized crime. Anvil is referenced in additional emails described below.

correspondent accounts held in the United States by United States banks between approximately November 3, 2010 and March 17, 2011.

- An account, [redacted] was used to send and to receive voluminous financial information concerning Zarrab-controlled companies (typically exchanging this information with the Al Nafees 99 Account) from at least in or about November 2011 through at least in or about June 2014. These emails include wire transfer confirmations and SWIFT messages, and accounting statements (such as trial balance statements, transaction ledgers, profit and loss statements, and deal registers). These financial records reflect, among other things, numerous transactions with counterparties located in Iran and transactions involving Iranian banks, including banks then-designated as SDNs by OFAC (such as Bank Melli, Bank Mellat, and Bank Saderat). The records also reflect billions of dollars of transactions in U.S. currency. For example, on or about November 18, 2012, the Al Nafees 99 Account emailed the [redacted] account portions of sub-ledgers for Al Nafees Exchange that appear to show aggregate U.S. dollar transactions (numbers and total amounts) for the years 2009, 2010, and 2011. These sub-ledgers indicate that Al Nafees Exchange purchased and sold approximately $722,298,309 and $722,206,314, respectively, in 2009; $1,912,116,577 and $1,912,203,188, respectively, in 2010; and $3,452,919,870 and $3,452,928,229, respectively, in 2011.

- On or about June 24, 2012, an email was sent from the Al Nafees 99 Account to the Central Bank of the United Arab Emirates stating, in part: “Kindly find the attachment (TT [wire transfers] TO USA FROM 01/01/2009 TO 30/06/2010).” Attached to the email was a spreadsheet reflecting approximately 806 wire transfers to U.S. beneficiaries. The remitter information in many of the transfers indicates an Iranian origin, such as transfers from Sepahan Exchange, an Iranian exchange house, or Kebriamanesh Trading, an Iranian trading company.

[redacted] This account, among other things, received an email dated July 20, 2011, attaching an invoice dated July 7, 2011, from Marun Petrochemical—an Iranian oil company that appears to be owned or controlled by the National Iranian Oil Company—relating to the sale of petroleum products to North Energy General Trading LLC—a Dubai company—totaling approximately $5,813,961 (with a corresponding total valued in UAE dirham). The invoice instructs that payment should be made to a dirham-denominated account held in the name of Anvil International General Trading at Emirates NBD. As described above, the Al Nafees 99 Account emails include an email dated May 29, 2011, sent to Zarrab’s account with the subject: “Anvil EUR account” and forwarding bank account information for Anvil International General Trading at Emirates NBD.

According to records provided by U.S. banks, between at least on or about January 1, 2007, and at least on or about May 21, 2015, U.S. banks processed at least approximately 181 transactions totaling at least approximately $105,884,394 in which Anvil International was a sending party, receiving party, or intermediary, including (i) a $2500 transfer on or about January 31, 2011, from North Energy General Trading identified as “Freight for con 80;”and (ii) transfers from Zarrab-related companies Kapital Kiymetli Madenler San Ve Ticaret, Asi

Kiymetli Madenler Sandi, and Pirlanta Kiymetli Madenler Sandi, between approximately December 2010 and February 2011 totaling approximately $94,717,165.70.

This information is in addition to the information the investigation already had obtained prior to the September 2014 warrants, which included publicly available information about Zarrab's involvement in billions of dollars' worth of gold trade with Iran and ton-quantity gold transactions with Babak Zanjani; evidence of Zanjani's massive sanctions evasion for the Iranian Ministry of Oil; evidence of international financial transactions totaling hundreds of millions of dollars through U.S. banks by Al Nafees Exchange and other Zarrab-related companies related to gold transactions or having unidentified purpose; evidence of international financial transactions through U.S. banks by Al Nafees Exchange and other Zarrab-related companies for Iranian individuals or entities; and evidence of email communications by Zarrab and others showing that their accounts likely contained communications related to these transactions.

Thus, wholly independent of the search of the defendant's email account, the Government was in possession of information and evidence overwhelmingly providing probable cause to search the defendant's account before and after September 2014. The record is clear, based on "demonstrated historical facts capable of ready verification," that the Government *would* in fact have relied on this evidence to seek and obtain a search warrant for the defendant's email account, among others. Even prior to seeking a warrant to search the defendant's account and others in September 2014, the grand jury had issued a subpoena for subscriber and other information concerning the defendant's account; the Government had obtained judicial authorization to install a pen register and trap-and-trace device with respect to the defendant's account; and the Government had obtained a court order for the production of header information for emails stored in the account. After reviewing the results of the September 2014 warrant and other evidence from the investigation, the Government *did* seek additional warrants for the contents of additional email accounts based on the emails obtained, not only from the defendant's account, but also from the other email accounts searched pursuant to the September 2014 warrants, including warrants for renewed searches of the defendant's account and a second account also controlled by the defendant in July 2015 and June 2016.

Accordingly, the Government inevitably would have obtained a warrant to search the defendant's email account, and the evidence should not be suppressed for this additional reason.

Respectfully submitted,

PREET BHARARA
United States Attorney

by: /s/
Michael D. Lockard/Sidhardha Kamaraju/
David W. Denton Jr., Assistant U.S. Attorneys
Dean C. Sovolos, Special Assistant U.S. Attorney
(212) 637-2193/6523/2744/2213

cc: All Defense Counsel (by ECF)